Wireless LAN Cardbus Adapter

User Manual

Version: 4.0
(June, 2004)

COPYRIGHT

Copyright © 2002/2003 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for Certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such a PDAs or lappads is not authorized. This transmitter is restricted for use with the specific antenna(s) tested in the application for Certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 INTRODUCTION 1

1.1 FEATURES 1
1.2 SPECIFICATIONS 1
1.3 PACKAGE CONTENTS 2

2 INSTALLATION PROCEDURE 3

2.1 INSTALL THE DRIVER 3
2.2 INSTALL THE UTILITY 5
2.3 USING UTILITY IN WINDOWS XP 7
2.3.1 Using the Windows XP's Utility 7
2.3.2 Using the Utility of this adapter 7

3 CONFIGURATION UTILITY 10

3.1 UTILITY OVERVIEW 10
3.2 CONNECT TO THE WIRELESS NETWORK 11
3.3 CONNECTION STATUS 12
3.4 PROFILE LIST 13
3.4.1 Configure the Profile 14
3.4.2 Enable WPA in Windows XP 16
3.5 ADVANCED CONFIGURATION 19
3.6 STATUS 21
3.7 STATISTICS 22
3.8 SOFTWARE AP 23
3.8.1 AP Connection Setting 23
3.8.2 AP Advanced Setting 24
3.8.3 Statistics 25

4 TROUBLESHOOTING 27

1 Introduction

Thank you for purchasing the Wireless LAN Cardbus Adapter. This adapter features the latest innovation wireless technology. For WLAN security issues, this adapter supports 64/128-bit WEP data encryption that protects your wireless network from eavesdropping. It also supports WPA (Wi-Fi Protected Access) feature that combines IEEE 802.1x and TKIP (Temporal Key Integrity Protocol) technologies. Client users are required to authorize before accessing to APs or AP Routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key. This adapter has built-in AES engine which ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. It also supports 32-bit cardbus interface which enables higher transmission performance. Furthermore, this adapter provides several kinds of power saving modes allowing user customizes the way of saving the power from his/her portable or handheld devices. This adapter is cost-effective, together with the versatile features, it is the best solution for you to build your wireless network.

1.1 Features

- Complies with the IEEE 802.11b (DSSS) 2.4GHz standard.
- High-speed transfer data rate - up to 11Mbps.
- Supports 64/128-bit WEP, WPA (TKIP with IEEE 802.1x)* and AES* functions for high level of security.
- Automatic fallback increases data security and reliability.
- Supports Software AP mode, which turns your adapter to a Wireless AP.
- Supports the most popular operating systems: Windows 98SE/Me/NT/2000/XP/Server 2003 and Linux*.
- Supports 32-bit Cardbus interface.

* Note:

1. WPA and AES functions are available in Windows XP.
2. Support Linux Kemel 2.4.18 (gcc version 2.96) and Kernel 2.4.20 (gcc version 3.2.2).

1.2 Specifications

- Standard: IEEE 802.11b
- Interface: 32-bit Cardbus
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps, DBPSK@1Mbps
- Radio Technology: Direct Sequence Spread Spectrum (DSSS)

- Data Rate: 11/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP Data Encryption, WPA (IEEE 802.1x with TKIP) and AES
- Antenna: Internal Antenna with Diversity System
- Drivers: Windows 98SE/Me/NT/2000/XP/Server 2003 and Linux
- LEDs: TX/RX, Link
- Power Voltage: 3.3V
- Transmit Power: 16dBm~18dBm
- Receive Sensitivity: -83dBm (Typical)
- Dimension: 5(H) x 115(W) x 54(D)
- Temperature: 32~131 ° F (0 ~55 ° C)
- Humidity: 0-95% (NonCondensing)
- Certification: FCC, CE, C-Tick, DGT

1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One Wireless Cardbus Adapter
- One CD (Driver/Utility/User' s Manual.)
- One Quick Guide

If any of the above items is missing, contact your supplier as soon as possible.

2 Installation Procedure

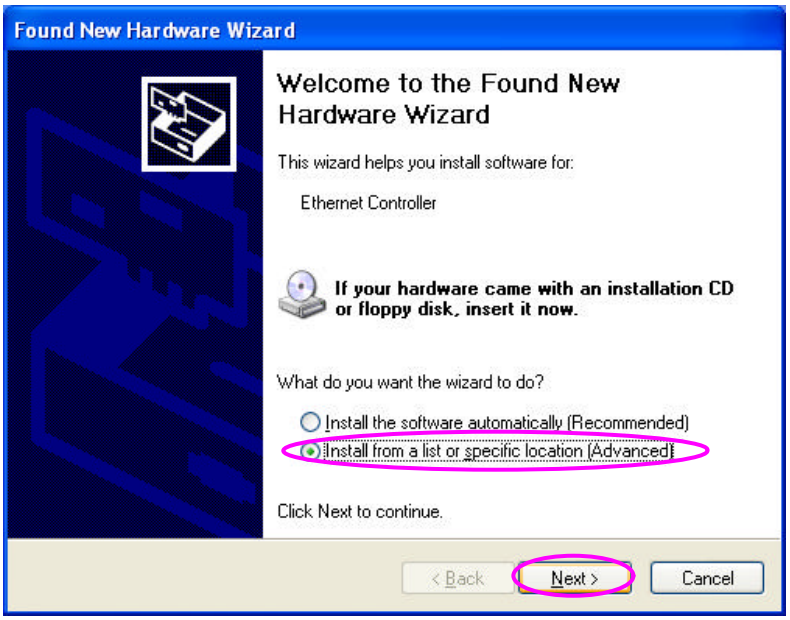
Before you proceed with the installation, please notice following descriptions.

Note1: The following installation was operated under Windows XP. (Procedures will be the same for Windows 98SE/Me/NT/2000/Server 2003.)

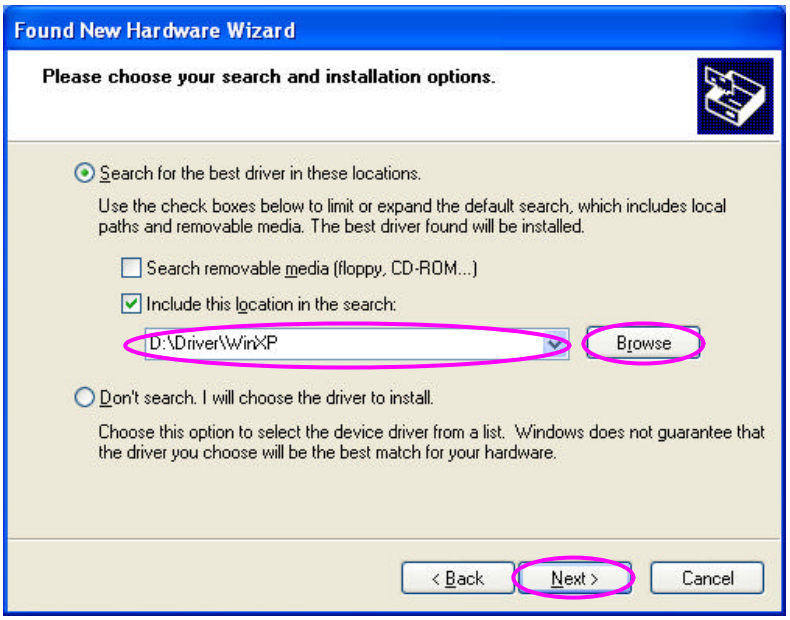
Note2: If you have installed the Wireless PC Card driver & utility before, please uninstall the old version first.

2.1 Install the Driver

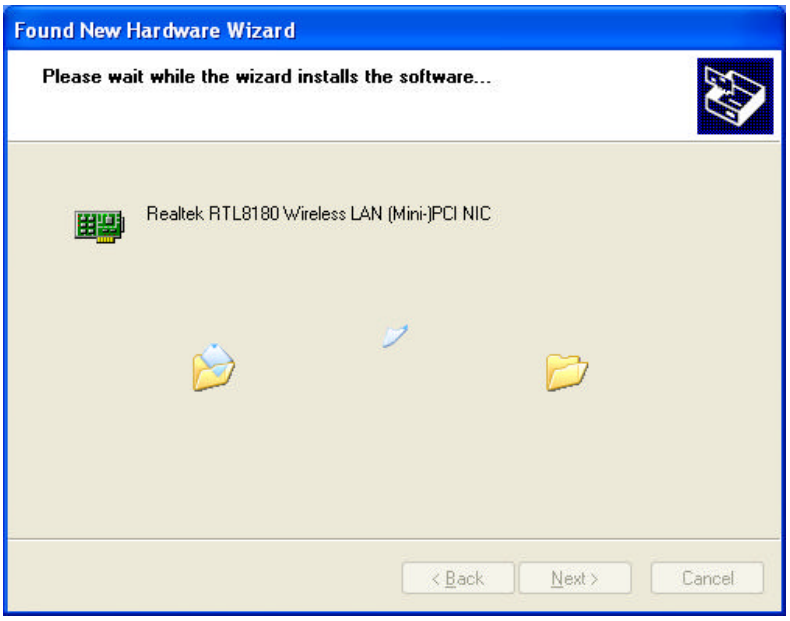
1. Insert the adapter into the Cardbus port of your computer, the system will automatically find the adapter. Select "Install from a list or specific location (Advanced), then click "Next".


Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install software for:
Ethernet Controller
If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)
Click Next to continue.
< Back
Next >
Cancel

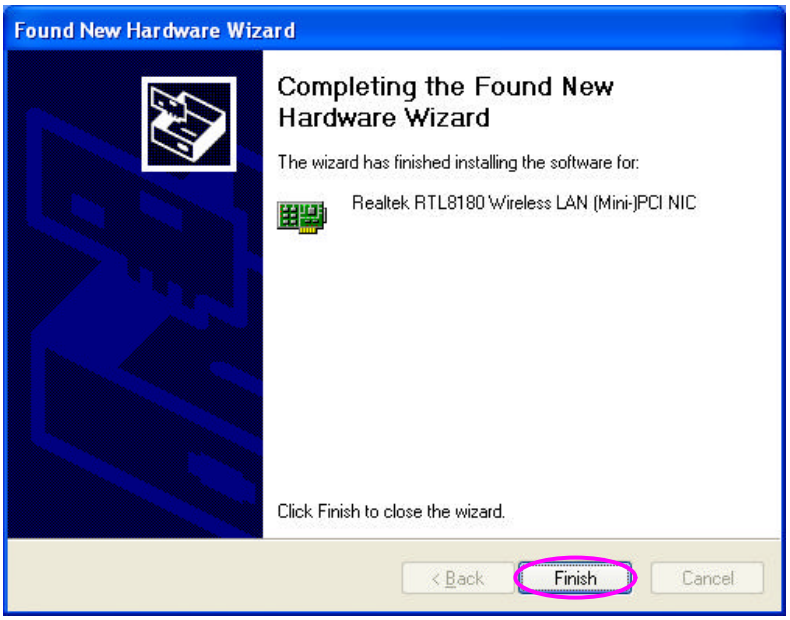
2. Click "Browser" to specify the driver from the CD attached with the adapter. For example, specify "D:\Driver\WinXP" folder (where "D" specifies your CD-ROM, the folder name is selected corresponding to your computer's OS system from the "Driver" folder of the CD). Click "Next".


Found New Hardware Wizard
Please choose your search and installation options.
Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
D:\Driver\WinXP
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.
< Back
Next >
Cancel

3. The system starts installing the driver for the adapter.

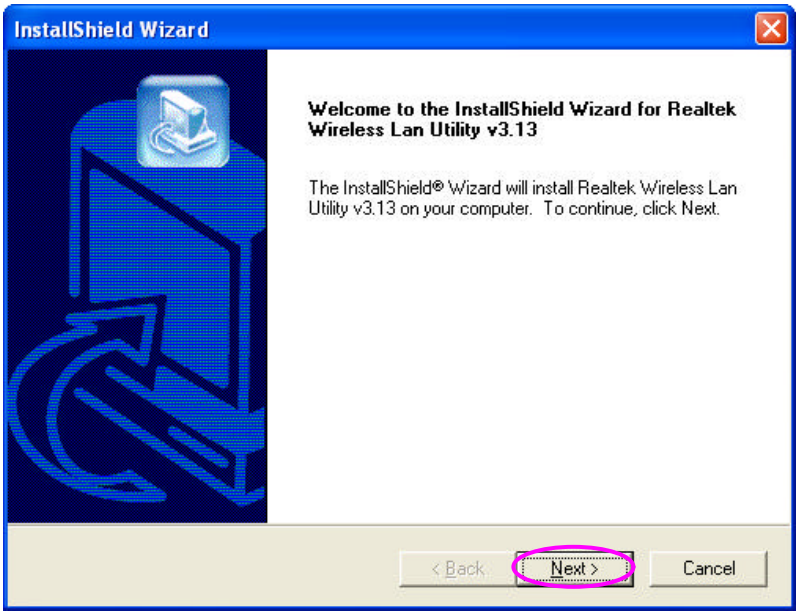

Found New Hardware Wizard
Please wait while the wizard installs the software...
Realtek RTL8180 Wireless LAN (Mini-)PCI NIC
< Back
Next >
Cancel

4. Click "Finish" when the installation is finished.

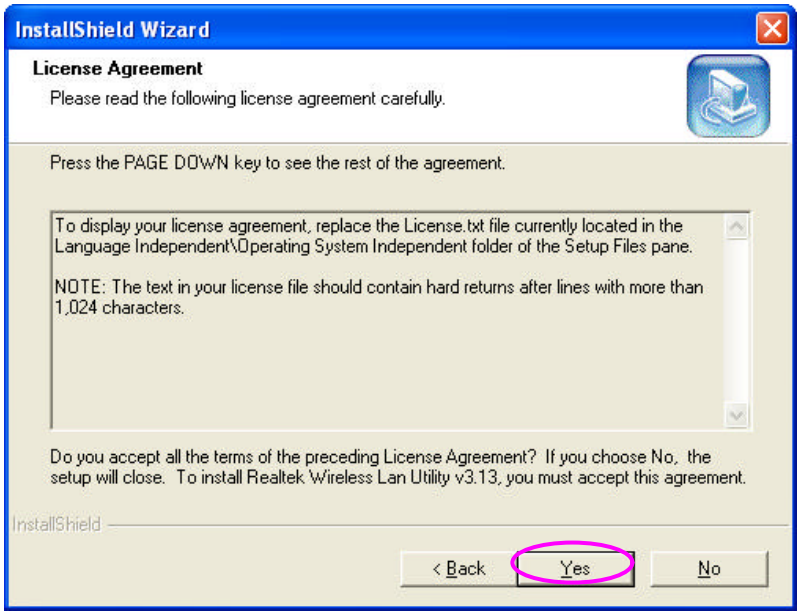

Found New Hardware Wizard
Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
Realtek RTL8180 Wireless LAN (Mini-)PCI NIC
Click Finish to close the wizard.
< Back
Finish
Cancel

2.2 Install the Utility

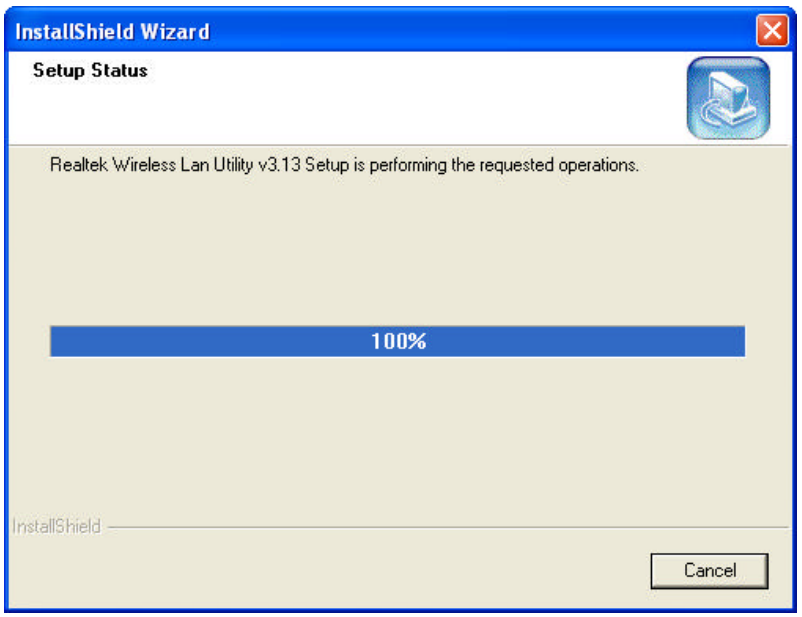
1. Insert the CD into the CD-ROM device and execute the "Utility\setup.exe" program. The InstallShield Wizard box will appear, click "Next" to continue.


InstallShield Wizard
Welcome to the InstallShield Wizard for Realtek Wireless Lan Utility v3.13
The InstallShield® Wizard will install Realtek Wireless Lan Utility v3.13 on your computer. To continue, click Next.
< Back
Next >
Cancel

2. Click "Yes" if you accept all the terms of preceding License Agreement.

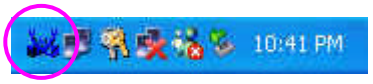

InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
To display your license agreement, replace the License.txt file currently located in the Language Independent\Operating System Independent folder of the Setup Files pane.
NOTE: The text in your license file should contain hard returns after lines with more than 1,024 characters.
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Realtek Wireless Lan Utility v3.13, you must accept this agreement.
InstallShield
< Back
Yes
No

3. The system will install the utility completely.



4. When you complete the Utility installation, a shortcut named "Rtl8180" will appear in the computer's desktop and a new icon will display in the system tray at the bottom of the screen. Double click the shortcut or the icon and start using the cardbus adapter.

In the Desktop



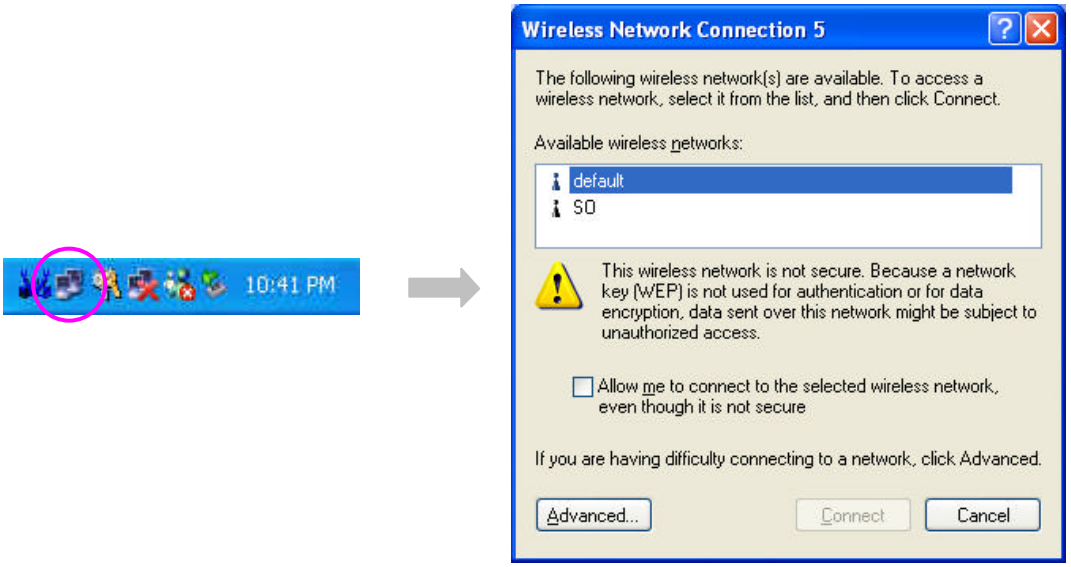
In the system tray

2.3 Using Utility in Windows XP

Due to the Windows XP has built-in wireless network utility (also known as wireless zero configuration) you may decide to use the "Windows Zero Configuration" or the one provided by this adapter. **If you don't disable the "Windows Zero Configuration", you couldn't connect to the selected network from the adapter's utility. It is strongly recommended to using the utility of this adapter.**

2.3.1 Using the Windows XP's Utility

Right click the icon marked in pink in the system tray and select "View Available Wireless Networks". You may start using the Windows XP's wireless utility.

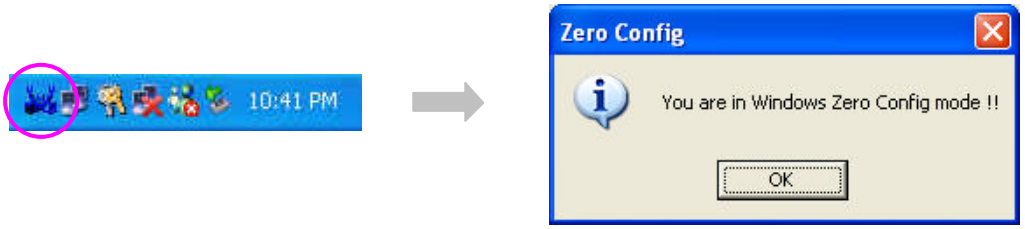

10:41 PM
Wireless Network Connection 5
The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.
Available wireless networks:
default
SO
This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.
Allow me to connect to the selected wireless network, even though it is not secure
If you are having difficulty connecting to a network, click Advanced.
Advanced...
Connect
Cancel

2.3.2 Using the Utility of this adapter

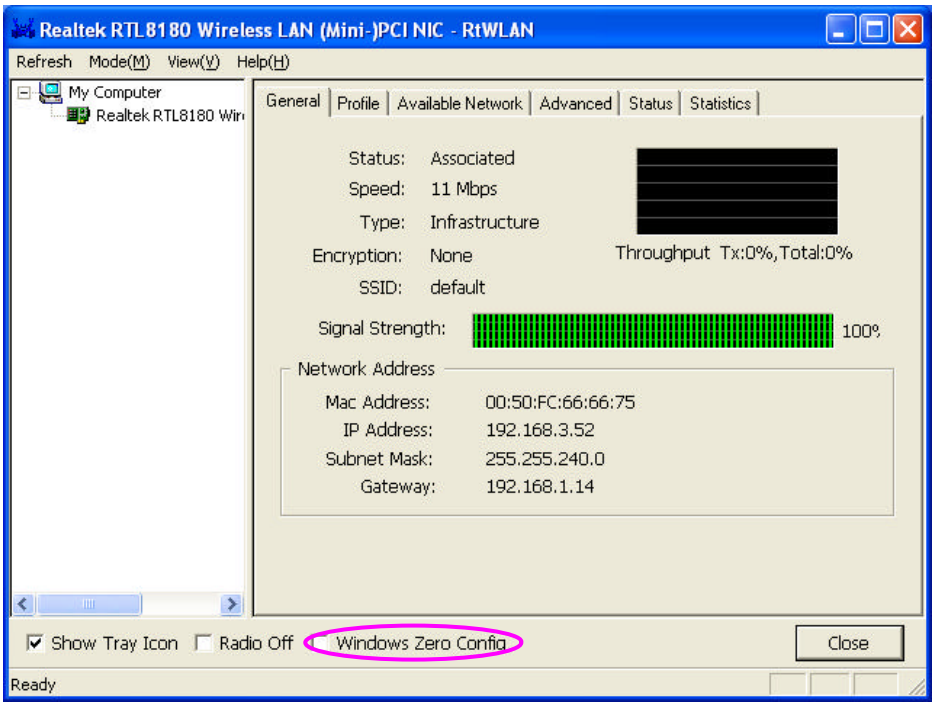
There are two ways to enable the utiility of the adapter.

First Way

1. Double-click the icon marked in pink in the system tray. A screen is popped up to remind you that you are using Windows Zero Configuration tool.

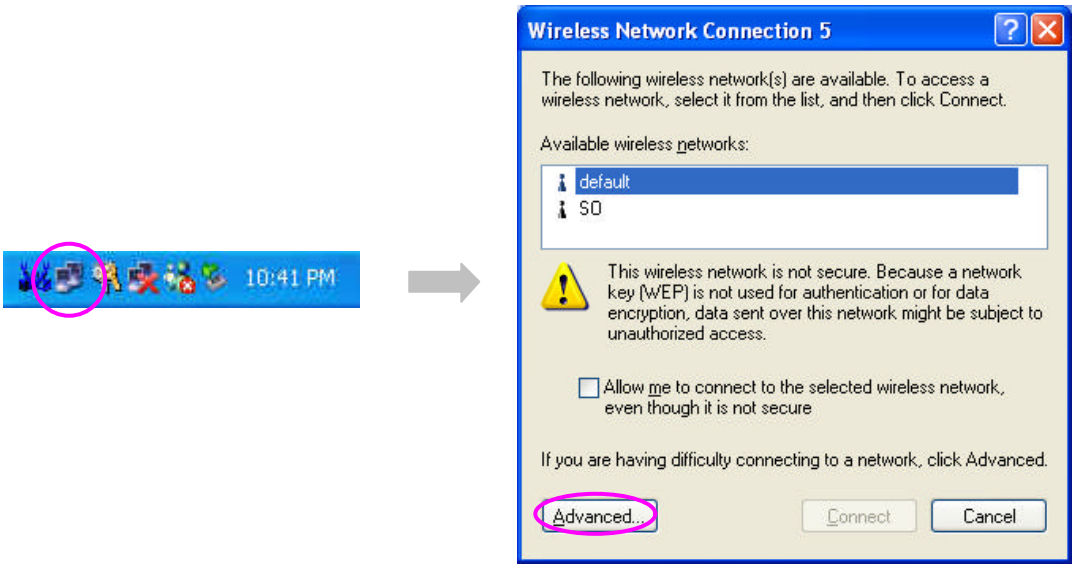


2. Clear the "Windows Zero Config" from the utility of the adapter.

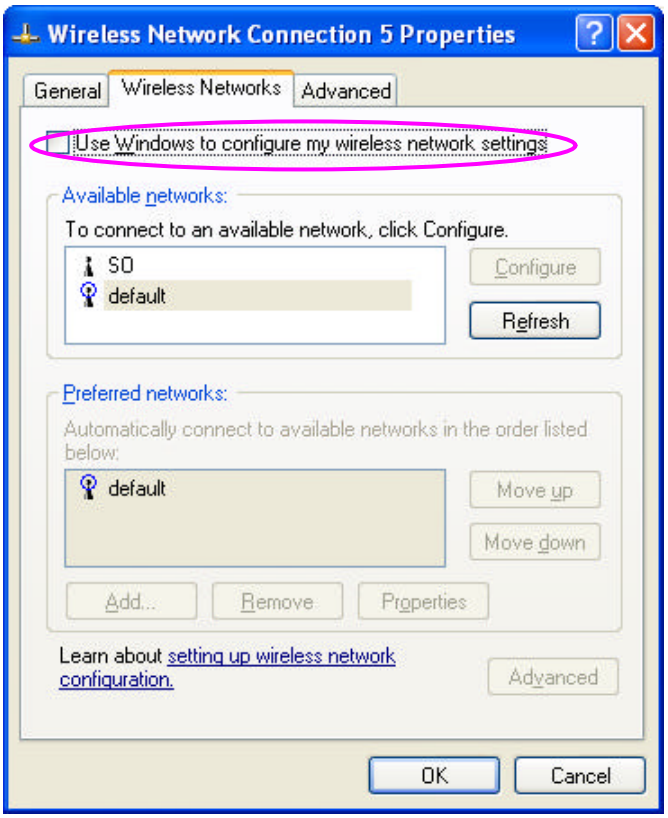


Second Way

1. Right click the icon marked in pink in the system tray and select "View Available Wireless Networks". Then, click "Advanced".


10:41 PM
Wireless Network Connection 5
The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.
Available wireless networks:
default
SO
This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.
Allow me to connect to the selected wireless network, even though it is not secure
If you are having difficulty connecting to a network, click Advanced.
Advanced...
Connect
Cancel

2. Clear the "Use Windows to configure my wireless network settings" check box.

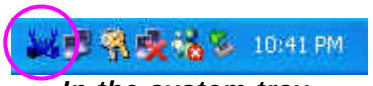

Wireless Network Connection 5 Properties
General
Wireless Networks
Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
SO
default
Configure
Refresh
Preferred networks:
Automatically connect to available networks in the order listed below:
default
Move up
Move down
Add...
Remove
Properties
Learn about setting up wireless network configuration.
Advanced
OK
Cancel

3 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the Wireless LAN Cardbus Adapter and monitor the link status and the statistics during the communication process.

The Configuration Utility appears as an icon on the system tray and desktop of Windows while the adapter is running. You can open it by double-click on the icon.

In the Desktop



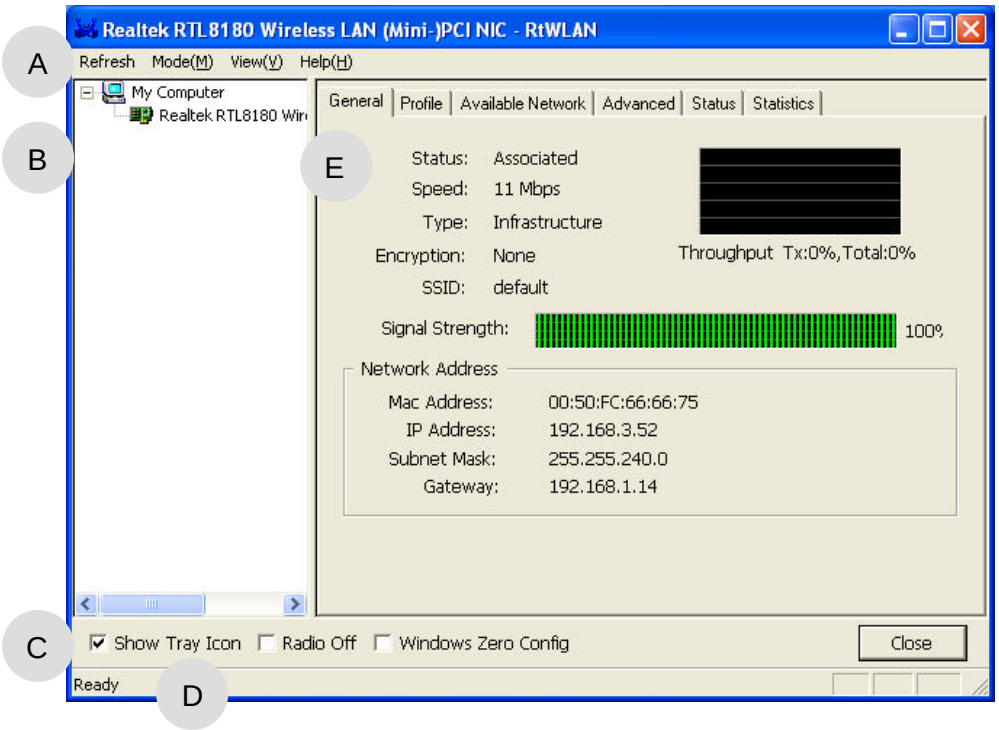
In the system tray

Right click the icon in the system tray, there are some items for you to operate the configuration utility.

- Close
  Close the Configuration Utility tool, the wireless connection is still active.
- About RTL8180
  Select "About RTL8180" to check the version of the tool.
- Config/Link Status
  Open the configuration tool.

3.1 Utility Overview

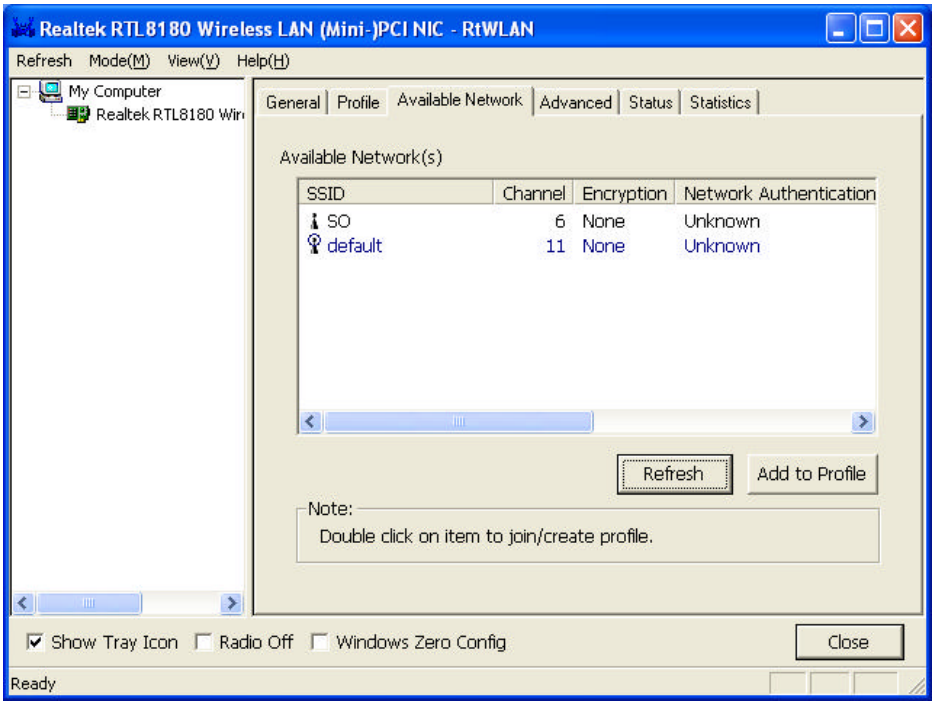
There are several parts in the utility screen. Please refer to the following table for the description.



Parameter	Description
A	**Refresh** – Refresh adapter list in the "B" block. **Mode** – There are two modes: Station and Access Point. If "Station" is selected, the adapter works as a wirelss adapter. If "Access Point" is selected, the adapter will works as a wireless AP. **View** – Check "Status Bar" and the "D" block in the utility will display the current status of the utility. **Help** – To check the version of the utility, select this item.
B	This is an adapter list for you to configure several adapters in your PC from the utility.
C	**Show Tray Icon** – To show the icon in the system tray, check the item. **Radio Off** – This function is for you to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work. **Windows Zero Config** – To configure the adapter from Windows XP Zero Configuration, check the item.
D	It is the status bar that displays the current status of the utility. To close it, please uncheck the "Status Bar" in the "View" item.
E	There are several tabs in the block for you to setup the function of the adapter. Please refer to the description in the following sections.

3.2 Connect to the Wireless Network

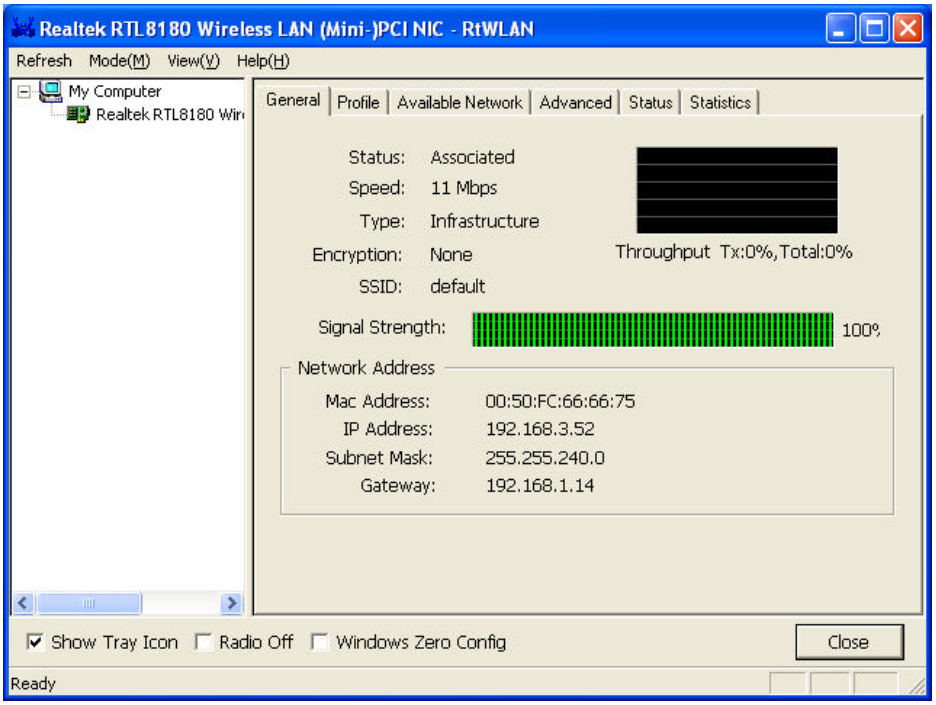
When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless network with the highest signal strength. From the "Available Network" tab, all the networks nearby will be listed. You can change the connection to another network.



Parameter	Description
Available Netowrk(s)	This list shows all information of the available wireless networks within the range of your adapter. The information includes SSID, Channel, Encryption and Singal, etc. If you want to connect to any network on the list, double-click the selected network.
Refresh	Click "Refresh" to update the available networks list. It is recommended that refresh the list while you have changed the connection network.
Add to Profile	A profile stores the setting of a network, so that you can connect to the network quickly. To add the selected network to a profile, click this button.

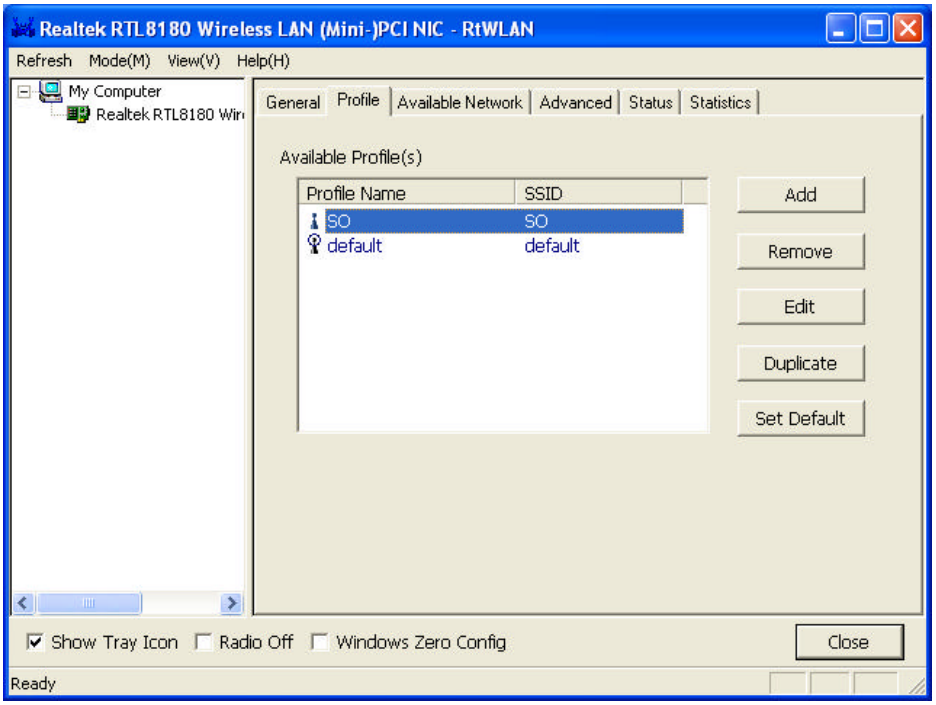
3.3 Connection Status

To check the connection status of the adapter, select "General". This screen shows the information of Link Speed, Network Type, Encryption Method, SSID, Signal Strength and Network Address of the adapter.



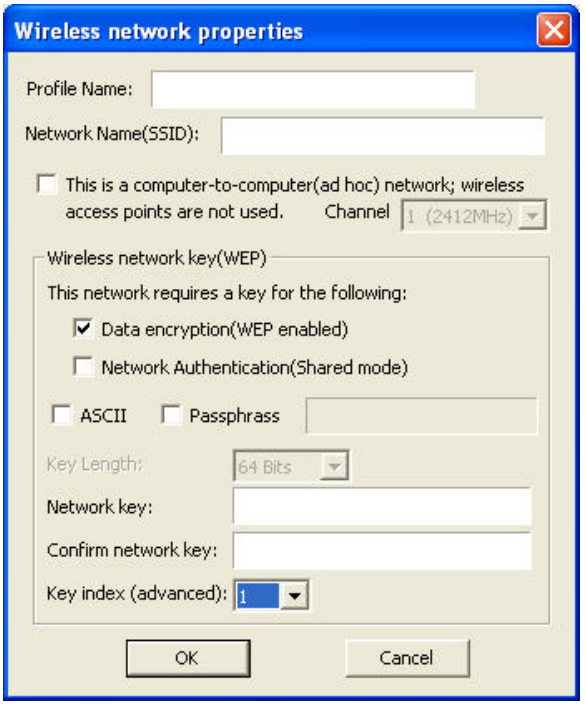
3.4 Profile List

This profile list shows all the profiles with its configurations currently stored in the program. You can click "Add", "Remove", "Edit", "Duplicate" and "Set Default" to configure the profile list.



Parameter	Description
Available Profile(s)	This list shows the preferred networks for the wireless connection. You can add, remove, edit, duplicate the preferred networks or set one of the networks as the default connection.
Add	To configurate a new profile, click "Add".
Remove	To remove a profile from the available profiles list, click "Remove".
Duplicate	To duplicate a profile with another name, click "Duplicate".
Set Default	To designate a profile as the default network for the connection from the available profiles list, click the button.

3.4.1 Configure the Profile



Parameter	Description
Profile Name	Define a recognizable profile name for you to identify the different networks.
Network Name(SSID)	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Only the wireless devices with the same SSID can interconnect.
This is a computer-to-computer(ad hoc) network....	There are two kinds of network type described as follows. **Infrastructure** – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. **Ad Hoc** – Connect to another wireless adapters in the Wireless LAN network without through an Access Point or Router. If this item is checked, the adapter will work in Ad Hoc mode.
Channel	This setting is only available for Ad Hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same with the network you are connecting to.
Wireless Network Key(WEP)	WEP is an data encryption algorithm, which protects authorized Wireless LAN users against eavesdropping. The security setting must be the the same on the wireless stations within the network.
Data Encryption(WEP Enabled)	To enable the WEP function, select the check box.
Network Authenticaton (Shared Mode)	The wireless network supports two subtypes of network authentication services: Open System and Shared Key. Under Open System authentication, any wireless adapters can request authentication. Under Shared Key authentication, only wirelss adapters using a shared key (WEP Key) are allowed to authenticate mutually. This network authentication mode setting has to be consistent with the wireless network which the adapter intends to connect.
ASCII	WEP Key can be ASCII format. Alphanumeric values or signs are allowed to be the WEP key. It is more recognizable for user.

Parameter	Description
Passphrase	It is a text string with a maximum of 32 alphanumeric characters, for example: "Test". The WEP Key are based upon the Passphrase determined by you. This passphrase may not work with other vendors' products due to possible incompatibility with other vendors' passphrase generators. You must use the same passphrase or WEP key settings for all wireless computers within the network.
Key Length	There are two kinds of key lengths: 64-bit and 128-bit. Larger key length will provide higher level of security, but the throughput will be lower.
Network Key	The keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. **64-bit** – Input 10-digit Hex values as the encryption keys. For example: "0123456aef". **128-bit** – Input 26-digit Hex values as the encryption keys. For example: "01234567890123456789abcdef".
Confirm Network Key	Enter the same network key to confirm.
Key Index(Advanced)	Select one of the four keys to be the data encryption key.

3.4.2 Enable WPA in Windows XP

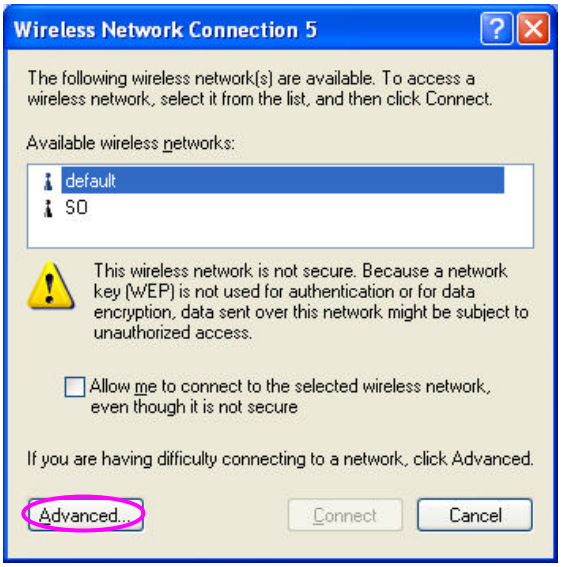
Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancement that strongly increases the level of data protection (encryption) and access control (authentication) for existing and future wireless LAN systems. The technical components of WPA include Temporal Key Integrity Protocol (TKIP) for dynamic key exchange, and 802.1x for authentication.

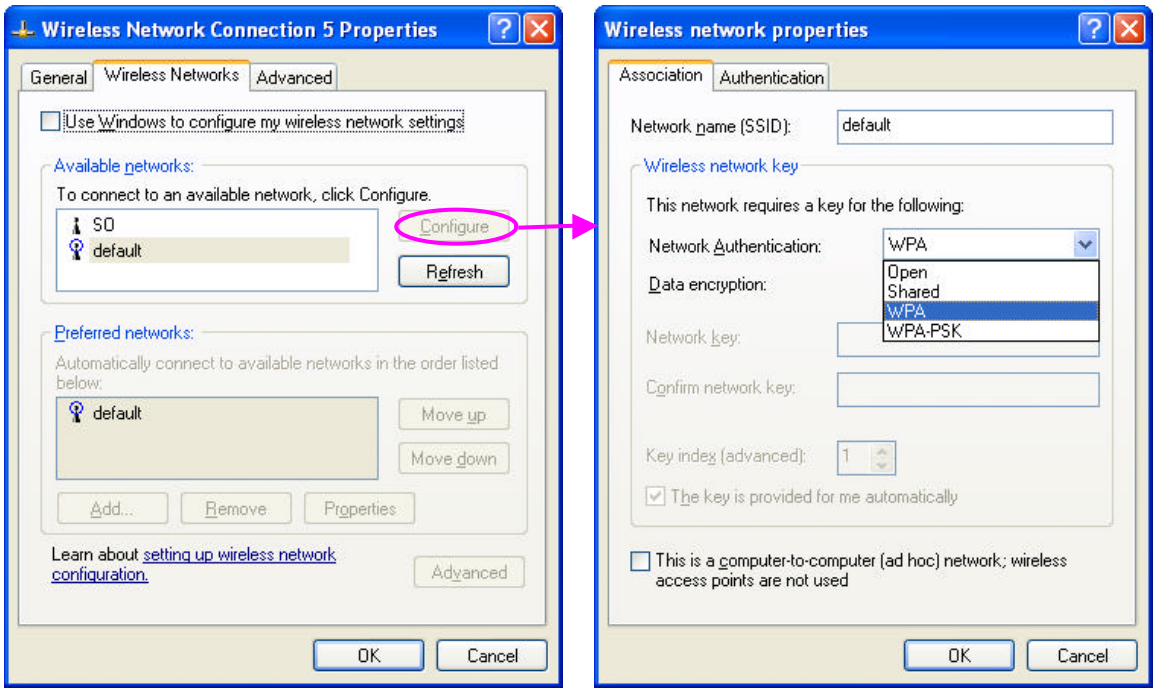
There are two types of WPA security: WPA-PSK (no server) and WPA (with server). WPA requires a Radius Server to complete the authentication among wireless adapters and Access Points. Typically, this mode is used in an enterprise environment. WPA-PSK uses a so-called pre-shared key as the security key. A pre-shared key is a password that each wireless station uses the same key to access the network. Typically, this mode will be used in a home environment.

To enable the WPA function in Windows XP, the following software systems are required:

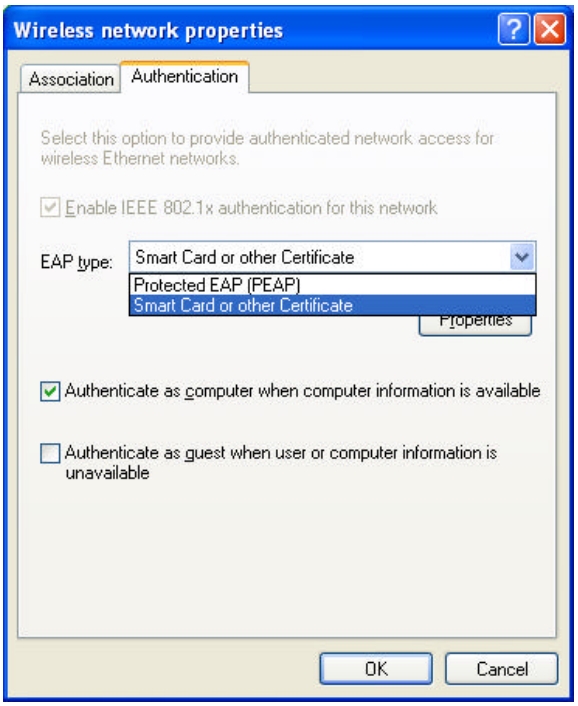
1. Windows XP Service Pack 1 with Windows XP Support Patch for Wi-Fi Protected Access program in addition.
2. Configure the adapter by Wireless built-in utility (Wireless Zero Configuration).

1. Right click the icon.
2. Select “View Available Wireless Networks“ and click “Advanced“.


Wireless Network Connection 5
The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.
Available wireless networks:
default
SO
This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.
Allow me to connect to the selected wireless network, even though it is not secure
If you are having difficulty connecting to a network, click Advanced.
Advanced...
Connect
Cancel



3. Click “Configure” button to configure the WPA function for the current network.

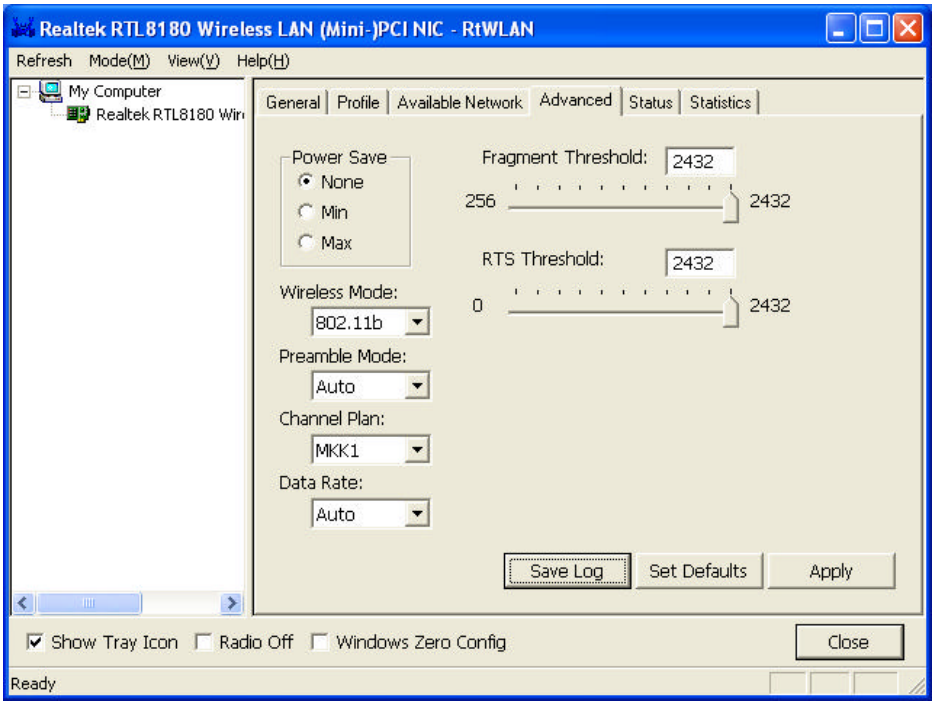

Wireless network properties
Association
Authentication
Select this option to provide authenticated network access for wireless Ethernet networks.
Enable IEEE 802.1x authentication for this network
EAP type:
Smart Card or other Certificate
Protected EAP (PEAP)
Smart Card or other Certificate
Properties
Authenticate as computer when computer information is available
Authenticate as guest when user or computer information is unavailable
OK
Cancel

Parameter	Description
Association	
Network Authentication	**Open** –No authentication is needed among the wireless network. **Shared** – Only wireless stations using a shared key (WEP Key identified) are allowed to connecting each other. **WPA** – This mode is for enterprise with an authentication server (Radius Server), WPA-enabled access point, and a WPA-enabled client. Once WPA is enabled, all adapters and access points on the network must be WPA-enabled in order to access the network. **WPA-PSK** – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each PC on the wireless network. WPA takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

Parameter	Description
Data Encryption	**WEP** – In WPA or WPA-PSK mode, WEP is also able to be the encryption method for the transmission data. **TKIP** – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. **AES** – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network. Note: All devices in the network should use the same encryption method to ensure the communication.
Association	
Enable IEEE 802.1x authenticatin for this network	If WPA or WPA-PSK authentication type is selected, IEEE 802.1x mode will be enabled automatically.
EAP Type	Select the protocols which is used to complete the authentication. For more setting, please check with your network administrator.

3.5 Advanced Configuration

This screen allows you to do some advanced configuration including Power Save Mode and some specific settings for the adapter.

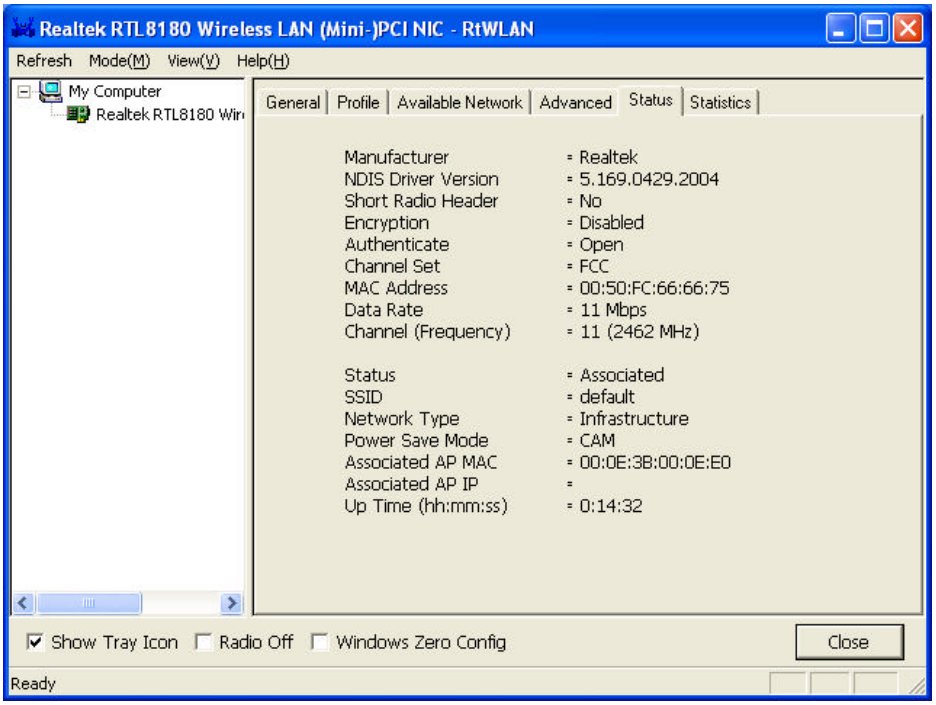


Parameter	Description
Power Save	**None** – Adapter will always set in active mode. **Min** – Enable the adapter in the power saving mode when it is idle, but some compoents of the adapter is still alive. In this mode, the power consumption is larger than "Max" mode. **Max** – Enable the adapter in the power saving mode when it is idle.
Wireless Mode	This adapter is an IEEE 802.11b wireless adapter.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If "Auto" mode is selected, the adapter will auto switch the preamble mode depending on the wireless stations which the adapter is connecting to. Note that the parameter is only active in the Ad Hoc operation mode.
Channel Plan	The available channel differs from different country. For example: USA is channel 1-11, Europe (ETSI) is channel 1-13. The channel of the adapter has been set depends on the country you are located. If you are in different country, you could change the channel from the pull-down list.

Parameter	Description
Data Rate	There are several options including Auto/1/2/5.5/11Mbps for you to select. When the "Auto" is selected, the adapter will choose the most suitable transmission rate automatically. The higher data rate you designated in the network, the shorter distance is allowed between the adapter and the APs or Routers.
Fragment Threshold	The value defines the maximum size of packets; any packet size larger than the value will be fragmented. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Select a setting within a range of 256 to 2432 bytes. Minor change is recommended.
RTS Threshold	Minimum packet size required for an RTS (Request To Send). For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the wireless network. Select a setting within a range of 0 to 2432 bytes. Minor change is recommended.
Save Log	Record the setting of the adapter.
Set Defaults	Let the setting values return to default.
Apply	Confirm the settings in the "Advanced".

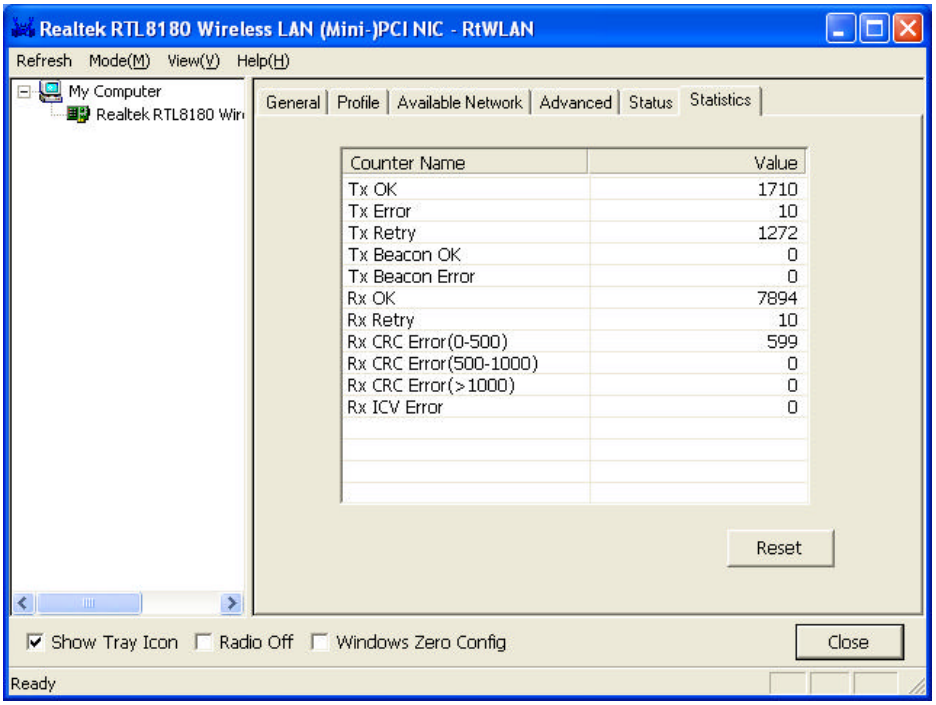
3.6 Status

This screen shows the information of manufacturer, driver version, settings of the wireless network the adapter is connecting to, linking time and link status. If you don't ensure the status of the adapter and the network you are connecting, please go to the screen for more details.



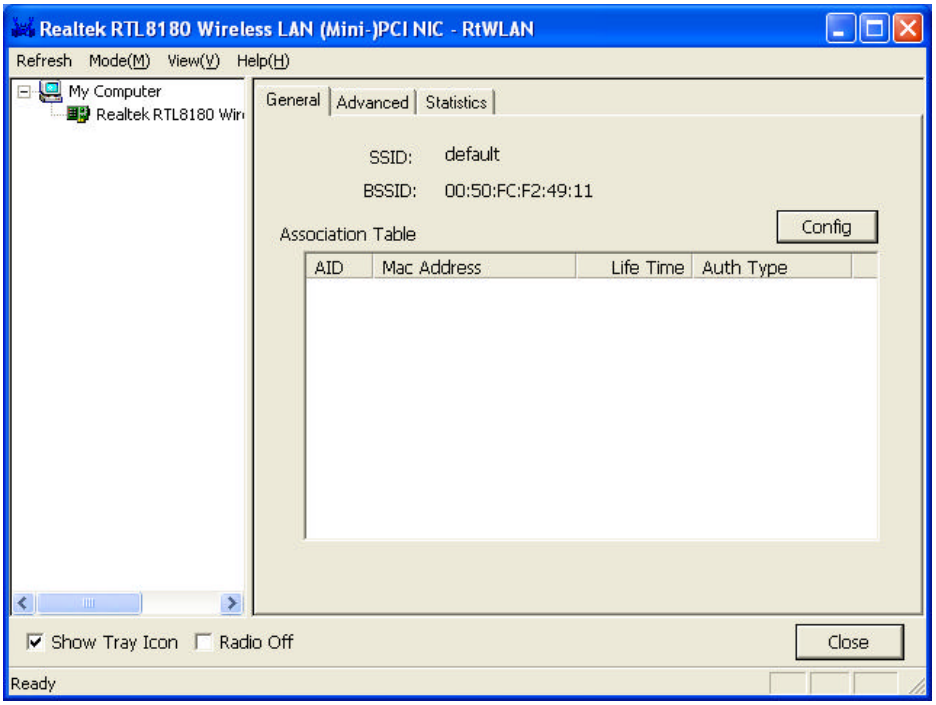
3.7 Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click " Reset".



3.8 Software AP

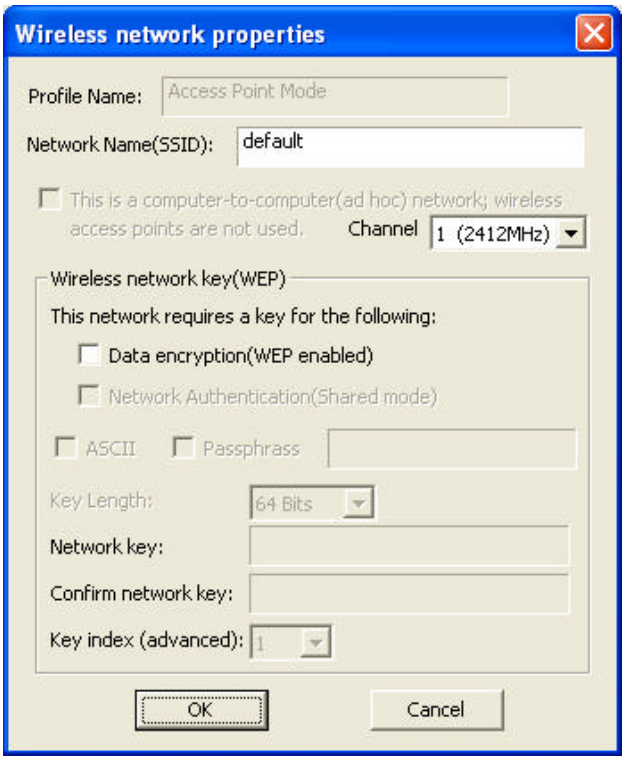
This adapter can run as a wireless AP. The relative configurations of the AP including channel, SSID, WEP encryption and so on are described as follows.



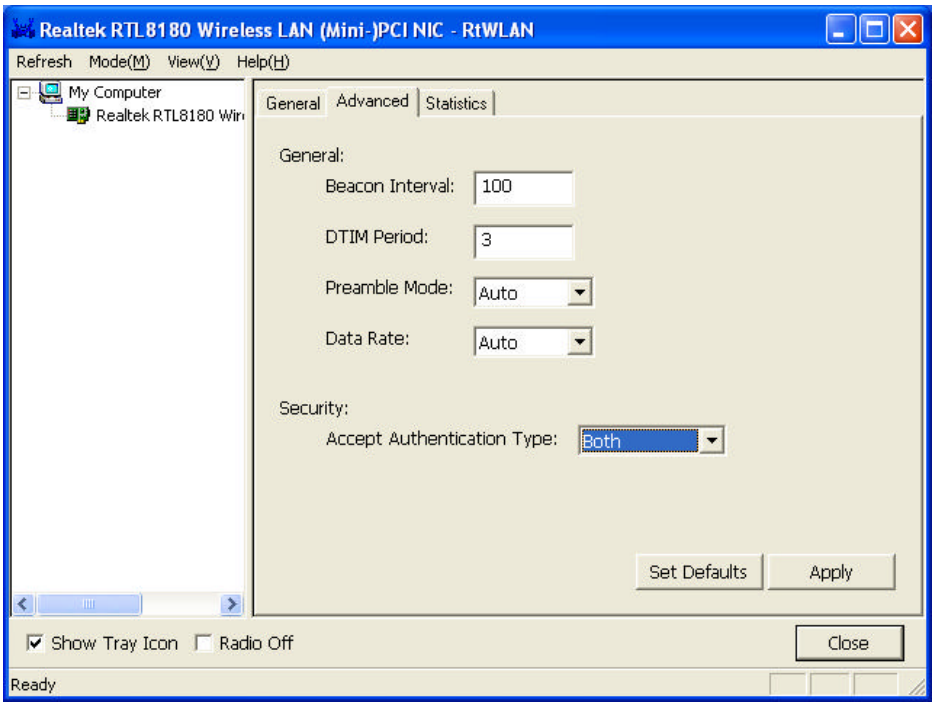
Parameter	Description
SSID	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the AP is "default". Wireless adapters connect to the AP should set up the same SSID as the AP.
BSSID	Display the MAC address of the adapter.
Associate Table	All the wireless adapters connected to the software AP will be dispalyed in the list.
Config	Click "Config" for setting more configuration of the AP.

3.8.1 AP Connection Setting

Please refer to Section 3.4.1 for the setting of the parameters for AP. Note that Ad Hoc mode is not enabled for AP.



3.8.2 AP Advanced Setting

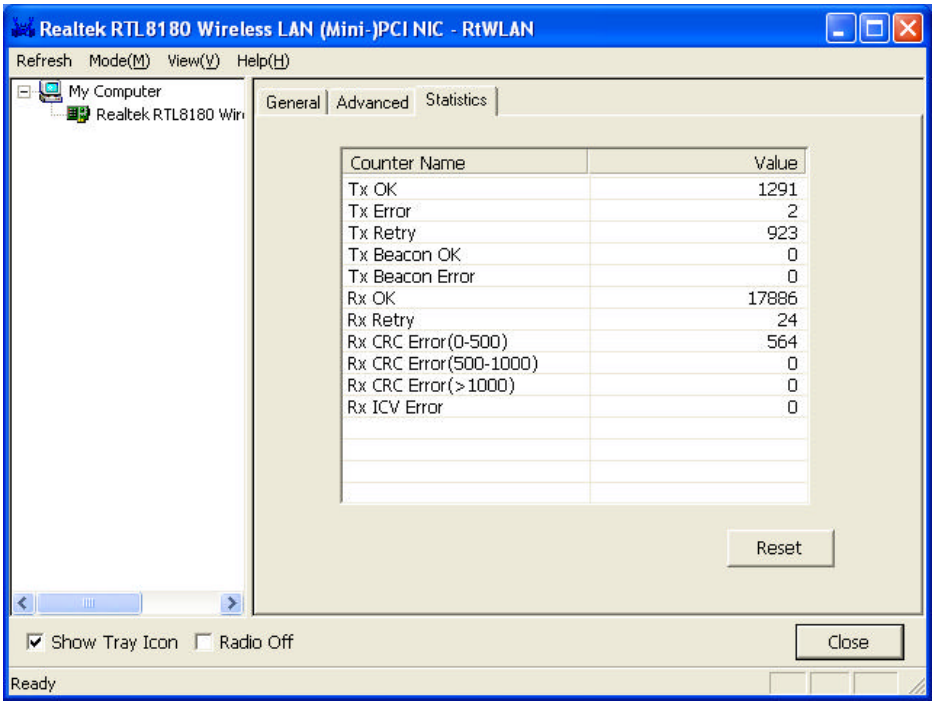


Parameter	Description
Beacon Interval	Beacon Interval which specifies the duration between beacon packets (milliseconds). The range for the beacon period is between 20-1000 milliseconds with a typical value of 100.

Parameter	Description
DTIM Period	Determines the interval the Access Point will send its broadcast traffic. Default value is 3 beacons.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are three mode including Long, Short and Auto. High network traffic areas should use the shorter preamble type. If "Auto" mode is selected, the AP will auto switch the preamble mode depending on the wireless adapters.
Data Rate	There are several options including Auto/1/2/5.5/11Mbps for you to select. When the "Auto" is selected, the AP will choose the most suitable transmission rate automatically.
Accept Authentication Type	The wireless network supports two subtypes of network authentication services: Open System and Shared Key. Under Open System authentication, any wireless adapters can request authentication. Under Shared Key authentication, only wirelss adapters using a shared key (WEP Key) are allowed to request authentication. If "Both" is selected, the AP can adjust the authentication type automatically.
Set Defaults	Let the setting values return to default.

3.8.3 Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from the screen. If you want to recount the statistics value, please click "Reset".


Realtek RTL8180 Wireless LAN (Mini-)PCI NIC - RtWLAN
Refresh
Mode(M)
View(V)
Help(H)
My Computer
Realtek RTL8180 Wir
General
Advanced
Statistics
Counter Name
Value
Tx OK 1291
Tx Error 2
Tx Retry 923
Tx Beacon OK 0
Tx Beacon Error 0
Rx OK 17886
Rx Retry 24
Rx CRC Error(0-500) 564
Rx CRC Error(500-1000) 0
Rx CRC Error(>1000) 0
Rx ICV Error 0
Reset
Show Tray Icon
Radio Off
Close
Ready

4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

1. What is the IEEE 802.11b standard?

The IEEE 802.11b Wireless LAN standard subcommittee which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

2. What does IEEE 802.11 feature support?

The product supports the following IEEE 802.11 functions:

- ●CSMA/CA plus Acknowledge Protocol
- ●Multi-Channel Roaming
- ●Automatic Rate Selection
- ●RTS/CTS Feature
- ●Fragmentation
- ●Power Management

3. What is Ad-hoc?

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

4. What is Infrastructure?

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

5. What is BSS ID?

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

6. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

7. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

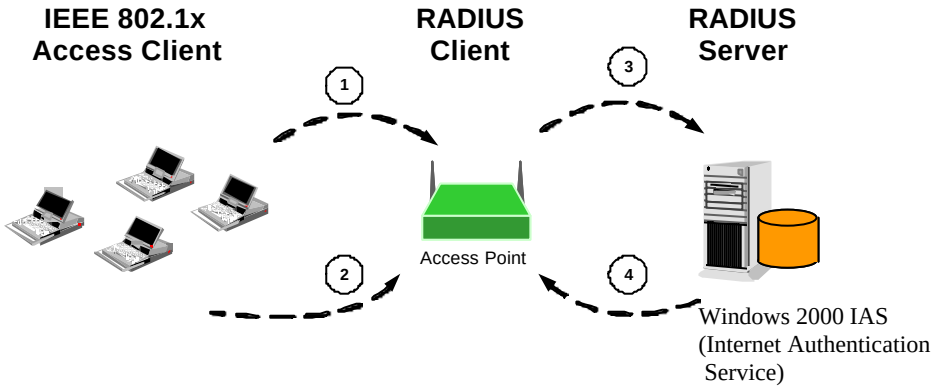
8. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

9. What is IEEE 802.1x?

802.1x, an IEEE standard that provides an authentication framework for 802-based LANs. 802.1x will let wireless LANs scale by allowing centralized authentication of wireless users or stations. Based on the 802.1x framework, any wireless stations try to connect to the Access Point or Router should be authenticated by an Authentication Server.

The Authentication Server identifies the wireless station by a set of user name and password, only wireless stations provide correct user name and password can connect to the Access Point or Router and access to the network.



(1) Client requests to login the network.

(2) Login with username, password.

(3) Send username, password to RADIUS server.

(4) Approve or deny user login to the LAN.

10. Can Wireless products support printer sharing?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS？What is FHSS？And what are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission**,** but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).